WHAT IS CLAIMED IS:

1. A method comprising:

sending a message from a client to a server, the message to establish a secure connection;

intercepting the data at a security system associated with the server to perform authentication functions; and

establishing a secure connection if proper authentications are performed.

2. The method of claim 1, wherein the proper authentications comprise determining if the server is authentic if the client has requested authentication.

3. The method of claim 2, wherein the proper authentications additionally comprise determining if the client is authentic if the server has requested authentication.

4. The method of claim 1, wherein said proper authentications comprise validating digital certificates.

5. The method of claim 1, additionally comprising decrypting the message if the message is encrypted.

6. The method of claim 1, wherein the authentication functions comprise:

the server requesting authentication from the client;

receiving a client certificate from the client; and

determining if the client is authentic, said determining occurring at the security system on behalf of the server.

7. The method of claim 6, wherein the message comprises a digital signature to validate the identity of the client, and said performing the proper authentications comprises validating the digital signature.

8. A method comprising:

receiving on a device associated with a server a client hello message from a client, the client hello message indicating a request to establish a secure connection with the server;

in response to the client hello message, the device sending a server hello message on behalf of the server to acknowledge the client hello message;

if authentication is requested by at least one of the client and the server, then exchanging authentication information;

sending a server hello done message from the device to the client, said sending being done on behalf of the server;

receiving a finished message from the client; and

sending a finished message to the client from the device, said sending being done on behalf of the server.

9. The method of claim 8, wherein said exchanging authentication information comprises:

if the client hello message includes a request for authentication from the server, then sending from the device authentication information to the client on behalf of the server; and

if the server requests authentication from the client, then receiving authentication information from the client.

10. The method of claim 8, wherein said sending a finished message to the client from the device on behalf of the server comprises:

determining if the client is authentic; and

if the client has been authenticated, then establishing a secure connection between the client and the server.

11. The method of claim 10, wherein the authentication information comprises a client certificate, and said determining if the client is authentic comprises validating the client certificate.

12. The method of claim 11, wherein validating the client certificate comprises determining that the client certificate is not on a certificate revocation list.

13. The method of claim 11, wherein the authentication information additionally comprises a digital signature, and said determining if the client is authentic additionally comprises verifying the digital signature.

14. The method of claim 8, additionally comprising decrypting the message if the message is encrypted.

15. An apparatus comprising:

an application module to:

receive incoming data sent from a client and destined for a given server of a plurality of servers in a data center; and

route the data to an authentication module to validate the identity of the client;

a wired device authentication module associated with the plurality of servers to:

receive the incoming data from the application module if the incoming data is sent using wired authentication information; and

authenticate the wired device;

a wireless device authentication module associated with the plurality of servers to:

receive the incoming data from the application module if the incoming data is sent using wireless authentication information; and

authenticate the wireless device;

a wired device decryption module associated with the plurality of servers to:

receive the incoming data from the application module if the incoming data is encrypted using a wired security protocol; and

decrypt the data to plain text; and

a wireless device decryption module associated with the plurality of servers to:

receive the incoming data from the application module if the incoming data is encrypted using a wireless security protocol; and

decrypt the data to plain text.

16. The apparatus of claim 15, wherein the wired device authentication module and the wireless device authentication module additionally support authentication functions for authenticating the given server by:

requesting server certificates from a certificate authority;

storing the server certificates; and

sending at least one of the server certificates to a client in response to the client's request for authentication.

17. The apparatus of claim 16, wherein the client is a wireless client, and said

sending comprises sending a long-lived certificate and a short-lived certificate to the wireless client.

18. The apparatus of claim 16, wherein said requesting server certificates from the certificate authority comprises requesting the server certificates at user-defined intervals.

19. A system comprising:

one or more servers to exchange data with clients; and

a security system associated with the one or more servers to:

support authentication functions for authenticating the identity of the one or more servers; and

authenticate the identity of clients requesting a secure connection with the one or more servers.

20. The system of claim 19, wherein said authentication functions for authenticating the identity of the one or more servers comprises:

requesting server certificates from a certificate authority; and

in response to a client requesting authentication from one of the one or more servers, sending a server certificate to the client.

21. The system of claim 19, wherein said authenticating the identity of clients requesting a secure connection with the one or more servers comprises:

updating a certificate revocation list (CRL);

receiving a client certificate from a client requesting a secure connection with a given one of the one or more servers associated with the security system;

determining if the client certificate is on the CRL; and

if the client certificate is on the CRL, then denying the client access to the given server.

22. An apparatus comprising:

a first means to:

receive incoming data sent from a client and destined for a given server of a plurality of servers in a data center; and

route the data to a means for validating the identity of the client by authenticating a device associated with the client;

a second means to:

receive the incoming data from the first means if the incoming data is sent using wired authentication information; and

authenticate the wired device;

a third means to:

receive the incoming data from the first means if the incoming data

is sent using wireless authentication information; and

authenticate the wireless device;

a fourth means to:

receive the incoming data from the first means if the incoming data is encrypted using a wired security protocol; and

decrypt the data to plain text; and

a fifth means to:

receive the incoming data from the first means if the incoming data is encrypted using a wireless security protocol; and

decrypt the data to plain text.

23. The apparatus of claim 22, wherein the second and third means additionally support authentication functions for authenticating the given server by:

requesting server certificates from a certificate authority;

storing the server certificates; and

sending at least one of the server certificates to a client in response to the client's request for authentication.

24. The apparatus of claim 23, wherein the client is a wireless client, and said sending comprises sending a long-lived certificate and a short-lived

certificate to the wireless client.

25. The machine-readable medium of claim 23, wherein said requesting server certificates from the certificate authority comprises requesting the server certificates at user-defined intervals.

26. A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

receive a message from a client to a server, the message to establish a secure connection;

intercept the data at a security system associated with the server to perform authentication functions; and

establish a secure connection if proper authentications are performed.

27. The machine-readable medium of claim 26, wherein the proper authentications comprise determining if the server is authentic if the client has requested authentication.

28. The machine-readable medium of claim 26, wherein the message comprises a client certificate to validate the identity of the client, and said performing the proper authentications comprises validating the client certificate.

29. The machine-readable medium of claim 26, wherein the authentication functions comprise:

the security system requesting authentication from the client on behalf of the server;

receiving a client certificate from the client; and

determining if the client is authentic, said determining occurring at the security system on behalf of the server.

30. An apparatus comprising:

at least one processor; and

a machine-readable medium having instructions encoded thereon, which when executed by the processor, are capable of directing the processor to:

receive a message from a client to a server, the message to establish a secure connection;

intercept the data at a security system associated with the server to perform authentication functions; and

establish a secure connection if proper authentications are performed.

31. The apparatus of claim 30, wherein the proper authentications comprise determining if the server is authentic if the client has requested authentication.

32. The apparatus of claim 30, wherein the message comprises a client

certificate to validate the identity of the client, and said performing the proper authentications comprises validating the client certificate.